REMARKS

The Examiner rejected claims 29, 30, 33, 35, 37, 39-41, and 47-49 under 35 U.S.C. 103(a) as being unpatentable over Le et al. (U.S. Patent 5,883,957) in view of Ghaibeh et al. (U.S. Patent 5,926,478).

Specifically, in response to the last amendment, the Examiner has now clarified the PTO's position with respect to the token element of the claims. The Examiner has indicated that the PTO's position is that the enabling bit string in Le correlates with the token of the presently claimed invention. Applicant thanks the Examiner for this clarification. However, the Applicant traverses this rejection for the following reasons.

The Token in Le is not stored in non-volatile memory in encrypted form

The "enabling bit stream" in Le is a string of bits indicating a function that an SPU can perform. Col. 7, line 66 - Col. 8, line 2. This string of bits is stored in a capability table, which is stored in non-volatile memory. However, the enabled bit stream is never stored in encrypted form in the non-volatile memory. Applicant believes that this may be confusing because there are several areas in Le where encryption is involved. However, the enabling bit stream is not encrypted when it is stored in non-volatile memory.

One of the areas where encryption arises in Le is that the functions enabled by the "enabling bit streams" include encryption. The enabled bit streams, for example, might include cryptographic functions that can be used to generate keys for secure communications. Col. 8, lines 2-8. This, however, is not the same as the enabling bit streams being encrypted themselves. This is described in FIG. 2 and FIG. 3 and the corresponding text of Le. In these figures, for example, a "1" in the first bit of the enabling bit string indicates whether the SPU is allowed to perform the function of generating SPU public and private key pair (FIG. 2 indicates the bit offset of 0 correspond to this function, and FIG. 3 shows an enabling bit stream containing a "1" in that bit). The fact that the enabled functions may include encryption/decryption does not mean that the string of bits indicating this fact is encrypted. Indeed, FIG. 3 clearly shows the bit stream as being unencrypted.

One of the other areas where encryption arises in Le is the encryption of the digital signature. The digital signature is used to determine whether an administrator is permitted to alter the capability table. This digital signature arrives from the administrator in encrypted form and thus must be decrypted. This process is described in Col. 11, lines 57-61. However, this digital signature is not the enabling bit stream the Examiner refers to as the "token," and thus the

encryption of this digital signature is irrelevant when it comes to determining whether Le teaches an encrypted token. Applicant additionally notes that the digital signature is never stored in non-volatile memory in Le, but is rather stored in the volatile memory of the computer that houses the SPU. This is described in Col. 11, lines 35-41.

The other area where encryption arises in Le is in the MD5 hashing of the enabling bit string. Specifically, Col. 11, lines 61-64 describe a step where the enabling bit string is retrieved from the non-volatile memory of the SPU and a hash value is computed from it using a secure hash function to obtain a hash value. However, while the Examiner may be arguing that the resultant hash value is now encrypted, this hash value is not stored in non-volatile memory but rather is stored in the volatile memory of the computer that houses the SPU. Col. 11, lines 35-41. This is done so that a comparison may be then made between the hash value and a hash value generated from the digital signature. If the hash values match, then the administrator is authorized to alter the capability table in the non-volatile memory. A new **unencrypted** enabling bit stream is then stored in the non-volatile memory (Col. 12, lines 11-22). At no time is an encrypted version of an enabling bit stream stored in non-volatile memory.

Since Le never teaches or suggests encrypting the enabling bit stream and storing the encrypted enabling bit stream in non-volatile memory, the reference fails to teach or suggest an element of the independent claims.

The combination of Le and Ghaibeh does not teach or suggest encrypting a token using a MAC address of the cryptographic feature enablement system

The Examiner admits that Le does not disclose encrypting the token using the MAC address of the system. The Examiner further argues, however, that Le discloses encrypting the token with a device ID and that the device ID is a system serial number. The Examiner then argues that Ghaibeh discloses that a MAC address is a unique device ID and that that it would have been obvious for one of ordinary skill in the art to use a MAC address as the device ID of Le, since it is always unique. The Applicant respectfully disagrees.

Contrary to what is stated in the Office Action, Le does not teach encrypting the token with a device ID. As stated above, the token in Le is not encrypted at all. But furthermore, the serial number in Le is used to simply verify whether the capability table is intended for the SPU to which it is attempting to be applied ("a capability table intended for one SPU cannot be used with another SPU. This feature is accomplished through the use of a device identification (device ID) field in the capability table, which contains information such as a unique serial number and/or model number. Unless the information contained in the device ID field matches

the corresponding information stored in a device's secure memory, the capability table cannot be successfully loaded into that device.", Col. 5, line 66 - Col. 6, line 8). In other words, the device ID is not used for encrypting anything, let alone a token. It is merely used to match capability tables with SPUs so as to not apply a capability table intended for a first SPU to a second SPU.

As such, Applicant does not believe that the combination of Le and Ghaibeh is relevant.

For the above reasons, Applicant respectfully asserts that independent claims 33, 35, 37, 39, 43 and 47 are in condition for allowance.

As to dependent claims 30, 40-41, 44-45, and 48-49, these claims are also patentably distinct from the cited references for at least the same reasons as those recited above for the independent claim, upon which they ultimately depend. These dependent claims recite additional limitations that further distinguish these dependent claims from the cited references. For at least these reasons, claims 30, 40-41, 44-45, and 48-49 are not anticipated or made obvious by the prior art and/or the official notice outlined in the Office Action.

Applicant believes that all pending claims are allowable and respectfully requests a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
BEYER WEAVER LLP

/Marc S. Hanish/
Marc S. Hanish
Reg. No. 42,626

P.O. Box 70250
Oakland, CA 94612-0250
408-255-8001